International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Design A Low-Latency Cryptography Based Viterbi Algorithm Architectures

P.Chandra Sekhar, Dr.K.Amit Bindaj

[1]M.Tech scholar, Dept of E.C.E, Sai Tirumala NVR Engineering College, Narasaraopet.
[2] Professor & H.O.D, Dept of E.C.E,Sai Tirumala NVR Engineering College, Narasaraopet.

ABSTRACT: *Basically, Viterbi algorithm [V.A] is used in many applications like satellite communication, cellular relay and wireless local area networks. This algorithm is mainly applied to the decoding conventional codes and also to automatic speech recognition and storage devices. In Viterbi algorithm architecture we are using error detection scheme which depends on the low complexity and low latency. The main advantage of this proposed system is that it gives reliable requirements and as well as performance degradation. Here we use three variants in the system which recomputed with the encoded operands. Now this system is modified by detecting the both transient and permanent faults [P.F] which are mixed with signature based methods. Here in this paper we are using instrumented decoder architecture for the purpose of extensive error detection assessments. For the purpose of bench mark we are implementing the both application specific integrated circuit and field programmed gate array. Depend upon the reliability objectives and performance degradation tolerance, the proposed system is utilized.*

KEY WORDS: Viterbi algorithm[V.A], permanent faults[P.F]

I.INTRODUCTION

The main intent of this Viterbi algorithm is to decode the convolution codes. Decoding of this algorithm is used in various applications like satellite communication, cellular and radio relay. Generally this Viterbi algorithm is implemented with serializer and deserializer constraints which have critical latency.

This serializer and deserializer are widely used in local area and synchronous optical networks. In the same way it is used in the magnetic storage systems like hard disk drive or digital video disk. This algorithm consists of possible number of states.

Branch metric unit (BMU), add-compare-select (ACS) and survivor path memory (SPM) are the three components of Viterbi algorithm. Coming to the branch metric unit, it produces the metrics which are corresponded to the binary trellis and all this process will depends upon the received signal. Next one is survivor path memory, it manage the paths and gives the decoded data as output. An add-compare-select component consists of feedback loops. By using the iteration schemes we can limit the speed of the system.

In the Viterbi decoder we are using M-step look ahead technique to break the iteration bound. Here the look head technique will combine the several trellises Step to one trellis step. Branch metric pre-computation technique will dominates the entire complexity of the system. For every two consecutive steps there are pipelined registers in the BMP. Add operation is performed before the saturation of trills but after the saturation of trills the add operation is followed by compare operation. In this compare operation we need a parallel path which consists of less metrics.

As discussed earlier that Viterbi algorithm is used in convolution codes, this convolution codes produces the output which degrade the accuracy of decoding. Basically, the errors will occur in digital systems because of logic delay, alpha particles. In the same way, in advanced process technologies the errors are obtained due to the device shrinking, reduce power supply voltages and higher operating frequencies. Here the energetic protons and electrons are obtained due to the cosmic rays in single transients. So to avoid these errors we use the error detection scheme. This error detection technique is used in hardware architecture with various domains.

Now, this proposed Viterbi architecture is divided into two approaches for measuring both area and power consumption. By using these approaches we should minimize the efficiency of degradations. After this process the signature based approach is followed to get the acceptable efficiency and in the same way to detect the errors that is permanent and transient errors we should use the encoded operands. Now to detect errors in the ACS we use the variants which are recomputed with shift operations(RESO).In the same way to get the less faults we use the recomputed with rotated operands. In the proposed Viterbi algorithm architecture we use the redundancy techniques. At last we conclude this proposed system in three contributions which are given below

- At first we proposed an error detection method for the proposed Viterbi decoder. By using this detection technique we can get high error coverage as well as the performance also boosted. Signature based approaches are used to recomputed the encoder operands.
- Now the proposed error detection technique is simulated and results are obtained in the bench marking. In bench marking we can observe the results of our simulation and reliability of our proposed structure.
- At last the proposed error detection Viterbi decoder is implemented on the application specific integrated circuit and field programmable gate array. From the results we can observe that the proposed architecture is used reliably.

II.PROPOSED RELIABLE ARCHITECTURES

As we know that the concurrent error detection techniques will produce the large power consumption and occupies large area. So to overcome this we are utilizing the encoded operands which are recomputed. In this number of errors are number of operands are used to detect the errors. Generally, here first we will apply the operands but coming to the recomputed step, we will apply the operands which are encoded. From the signature based scheme the both transient and permanent errors are detected. Let us discuss about this proposed system in detail.

a) Unified Signature-Based Scheme For CSA And PCSA Units Within BMP:

To get the faster operation in ACS structure we should employ the parallelization of add and compare operations. Here the channel response is extended by an extra bit by doubling the number of states. In p-level parallelism, for k-1 step there is no compare operation but for M-K+1 step the add operation is followed by the compare operation. From this step we can eliminate the parallelism.

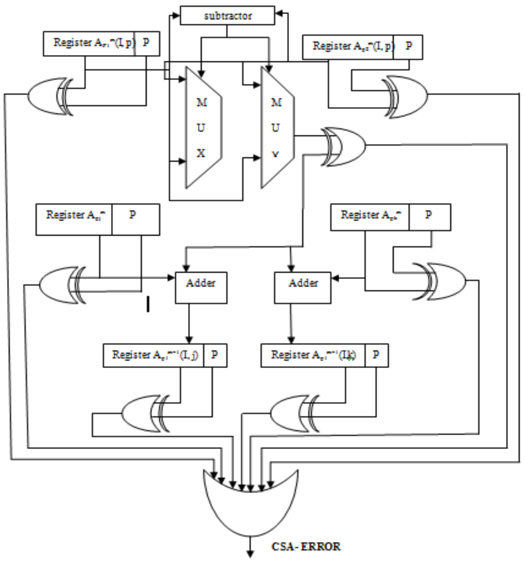


Fig. 1. The CSA signature-based error detection approach (the shaded adders are the types of the original ones with the proposed error detection schemes).

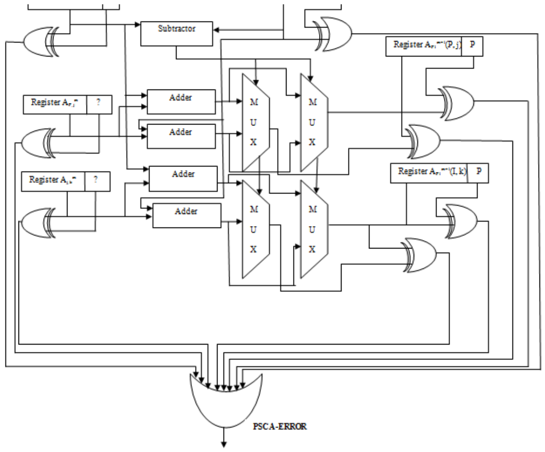


Fig. 2. Signature-based PCSA error detection (the shaded adders include the proposed error detection schemes).

The both add and compare operations are should be performed sequentially. But in our proposed algorithm the order of add and compare operations are changed to compare-add operations. This can be attributed as carry-select-add unit (CSA).The main purpose behind using this operation is to optimize the speed.

Now let us utilize the signature prediction schemes for the both CSA and PCSA units. Signatures are employed to all the registers in our proposed system. The below figure (1) and figure (2) shows the CSA and PCSA signature based error detection techniques. Here in CSA there is only single multiplexer and in PCSA there are two multiplexer. By using XOR gate the both original and duplicated multiplexers are compared and the output of XOR gate is connected to the input of OR gate. The input and output registers are incorporated with the signatures like single bit and multiple bits to detect the faults. To derive the error indication flags we use an OR gate. This OR gate will increase the number of error indication flags to detect the errors.

The both CSA and PCSA are the self-checking adders. Basically, self-checking adder's size is obtained by cascading the adders. This self-checking adder consists of five two-pair two-rail checkers and also four full adders and two multiplexers which are repeated by n-times. By using the XNOR gate the self-checking operation is performed. The checker consists of two pair of inputs which are driven from the fault-free scenario and they produce two outputs from the checker which is in the form of two-rail. Here if one of the input have fault then it does not produces output in two-rail form.

To overcome that a new self-checking adder is proposed for both CSA and PCSA. To increase the efficiency and performance of this system, we are using n-bit ripple carry adder. This ripple carry adder will re-compute the sum bits in carry-in by using complemented values. But to select the actual sum bits we use the original value of carry-in.

b) Re-computing With Encoded Operands for CSA and PCSA: Here by using the encoded operands they are RESO, RERO and variants of RERO, the error detection CSA and PCSA architectures are designed. Here to divide the time into sub parts, the pipeline registers are added to the sub-pipeline registers. During the first cycle the original operands will be obtained and during second cycle, the first half of the circuit is fed to the rotated operands and the second half of the circuit operates on the original operands. For the both CSA and PCSA we are employing the RESO and RERO operand. Here the RESO will perform the re-computation step with shifted operands. RERO is used to detect the errors.

III. RESULTS

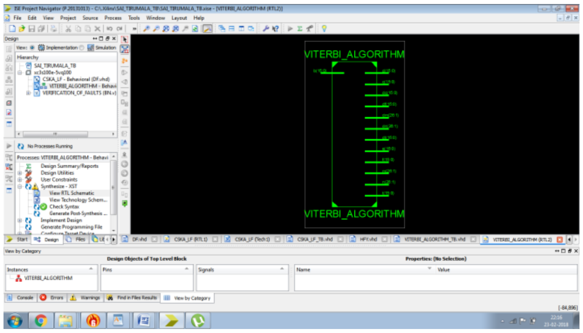


Fig 3. RTL Schematic

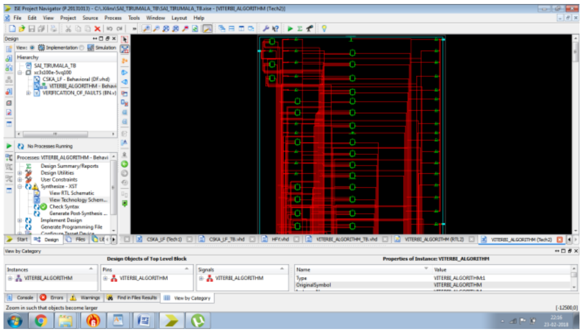


Fig 4. Technology Schematic

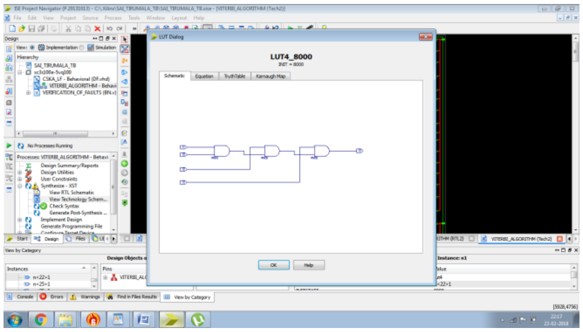
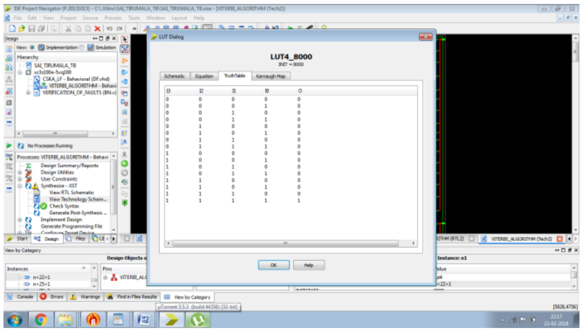


Fig 5. Look Up Table (LUT)



LUT4_8000
INIT = 8000

I3	I2	I1	I0	O
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	1

Fig 6. Truth Table

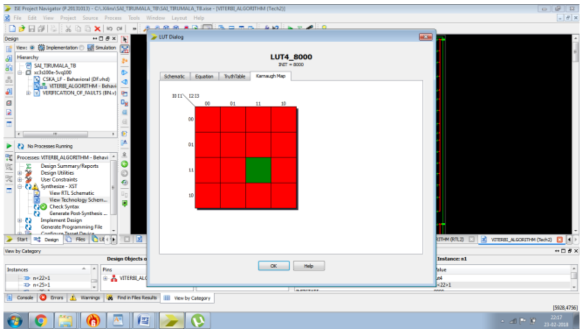
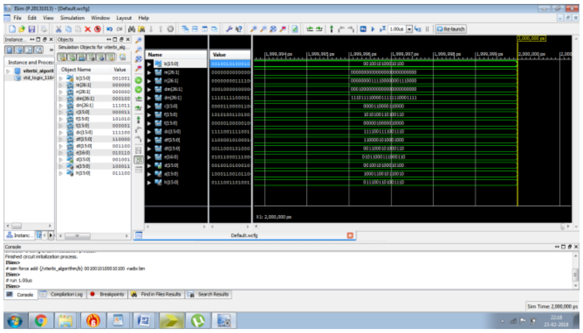


Fig 7. KMAP



```
Finished circuit initialization process.
ISim>
# isim force add {/viterbi_algorithm/b} 0010010100010100 -radix bin
ISim>
# run 1.00us
ISim>
```

Fig 8. Output Waveform

IV.CONCLUSION

In this paper we proposed error detection techniques for CSA and PCSA structures. These structures produce the low complexity and low latency Viterbi decoder. The proposed structure depends upon the signatures and various variant operands. The simulation results of the CSA and PCSA structures gives very high fault coverage. The both ASIC and FPGA are implemented to obtain better results which are acceptable. At last we can conclude that the proposed structure will be good reliability compared to the existed system.

V. REFERENCES

[1] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Trans. Inf. Theory*, vol. IT-13, no. 2, pp. 260–269, Apr. 1967.

[2] R. Liu and K. Parhi, "Low-latency low-complexity architectures for Viterbi decoders," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 56, no. 10, pp. 2315–2324, Oct. 2009.

[3] K. K. Parhi, *VLSI Digital Signal Processing Systems: Design and Implementation*. Hoboken, NJ, USA: Wiley, 1999.

[4] G. Fettweis and H. Meyr, "Parallel Viterbi algorithm implementation: Breaking the ACS-bottleneck," *IEEE Trans. Commun.*, vol. 37, no. 8, pp. 785–790, Aug. 1989.

[5] V. Gierenz, O. Weiss, T. Noll, I. Carew, J. Ashley, and R. Karabed, "A 550 mb/s radix-4 bit-level pipelined 16-state 0.25-μm CMOS Viterbi decoder," in *Proc. IEEE Int. Conf. Appl.-Specific Syst. Archit. Process.*, Jul. 2000, pp. 195–201.

[6] P. J. Black and T. H. Meng, "A 140-Mb/s, 32-state, radix-4 Viterbidecoder," *IEEE J. Solid-State Circuits*, vol. 27, no. 12, pp. 1877–1885, Dec. 1992.

[7] T. Gemmeke, M. Gansen, and T. Noll, "Implementation of scalable power and area efficient high-throughput Viterbi decoders," *IEEEJ. Solid-State Circuits*, vol. 37, no. 7, pp. 941–948, 2002.

[8] A. Yeung and J. Rabaey, "A 210 Mb/s radix-4 bit-level pipelined Viterbi decoder," in *Proc. IEEE Conf. Int. Solid-State Circuits*, Feb. 1995, pp. 88–89.

[9] K. Arunlal and S. Hariprasad, "An efficient Viterbi decoder," Int. Journal of Advanced Information Technology, vol. 2, no. 1, Feb 2012.

[10] J. Kong and K. Parhi, "K-nested layered look-ahead method and architectures for high throughput Viterbi decoder," in Proc. IEEE Workshop on Signal Processing Systems, 2003, pp. 99 – 104.

[11] G. Jung, J. Kong, G. Sobelman, and K.Parhi, "High-speed add-compare-select units using locally self-resetting CMOS," in IEEE Int. Symp.Circuits and Systems, vol. 1, 2002, pp. 889–892.

[12] K. K. Parhi, VLSI Digital Signal Processing Systems: Design and Implementation. Wiley, 1999.

[13] G. Fettweis and H. Meyr, "Parallel Viterbi algorithm implementation: Breaking the ACSbottleneck," IEEE Trans. Commun., vol. 37, no. 8, pp. 785 – 790, 1989.

[14] V. Gierenz, O. Weiss, T. Noll, I. Carew, J. Ashley, and R. Karabed, "A 550 Mb/s radix-4 bit-level pipelined 16-state 0.25-um CMOS Viterbi decoder," in Proc. IEEE Int. Conf. Appl.-Specific Syst., Archit. Process, 2000, pp. 195 – 201.

[15] P. Black and T. H. Meng, "A 140-Mb/s, 32-state, radix-4 Viterbi decoder," IEEE J. SolidState Circuits, vol. 27, no. 12, pp. 1877 – 1885, 1992.

[16] T. Gemmeke, M. Gansen, and T. Noll, "Implementation of scalable power and area efficient high-throughput Viterbi decoders," IEEE J. Solid-State Circuits, vol. 37, no. 7, pp. 941 – 948, 2002.

[17] A. Yeung and J. Rabaey, "A 210 Mb/s radix-4 bit-level pipelined Viterbi decoder," in Proc. IEEE Int. Solid-State Circuits Conf, 1995, pp. 88 – 89.

[18] K. Parhi and J. J. Kong, "Low-latency architectures for high-throughput rate Viterbi decoders," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 12, no. 6, pp. 642 – 651, 2004.

[19] H. Bar-El, H. Choukri, D. Naccache, and M. Tunstall, "The sorcerer's apprentice guide to fault attacks," IEEE Proceedings, vol. 94, no. 2, pp. 370 – 382, Jan 2006.

[20] M. Karpovsky and A. Taubin, "New class of nonlinear systematic error detecting codes," IEEE Trans. Information Theory, vol. 50, no. 8, pp. 1818 – 1819, July 2004

Dr K AMIT BINDAJ, PhD from Jodhpur National University, Jodhpur, Recg. by Govt. of Rajasthan. Presently working as H.O.D and Dean R &D , ECE in SaiTirumala NVR Engineering college , Narasaraopeta, having a Teaching experience of almost 14 years. His area of research is emerging Wireless communication Technology, 4GLongTerm Evaluations (LTE-A) and also ICT enabled services. He has also attended and conducted about dozen of workshops and FDP. He presented & published the Research Papers in almost more than dozen of National and International conferences and High impact factor International Journals.

P.CHANDRA SEKHAR completed his B.Tech Amara Inistitute of Engineering And Technology and pursuing M.TECH in Sai Tirumala NVR Engineering College.